MPTCP および製品サポートの概要

内容

概要

このドキュメントでは、マルチパス TCP（MPTCP）の概要、フロー インスペクションに対する影響、この影響を受けるシスコ製品と影響を受けないシスコ製品について説明します。

MPTCP の概要

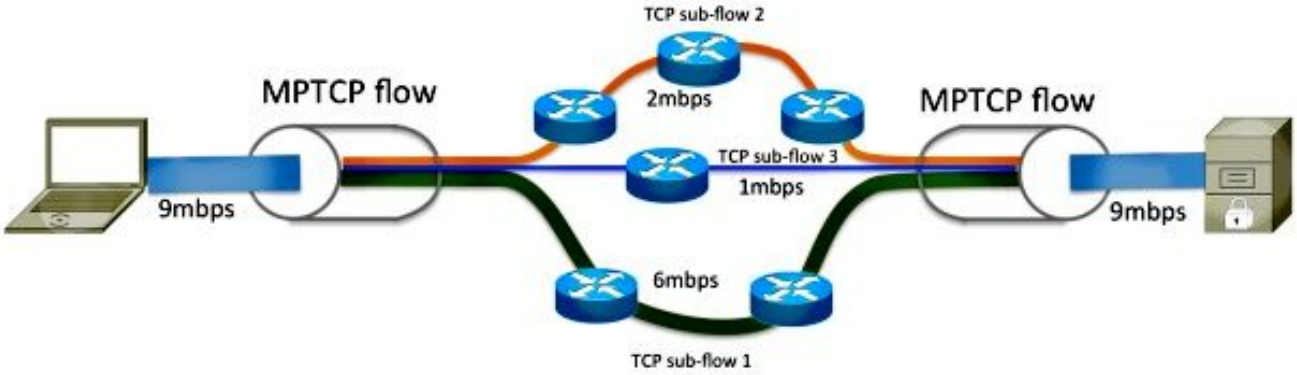
背景説明

インターネットに接続されたホストまたはデータセンター環境内のホストは通常、複数パスによって接続されます。ただし、TCP をデータ転送に使用している場合、通信は単一のネットワークに制限されます。代替パスが十分に利用されない場合、2 台のホスト間で複数のパスが輻輳することが可能です。これらの複数のパスが同時に使用されることで、ネットワーク リソースを効率的に使用することができます。また、複数の接続を使用することにより、ネットワーク障害に対するより高いスループットと改善された復元力が可能になるため、ユーザ エクスペリエンスが向上します。

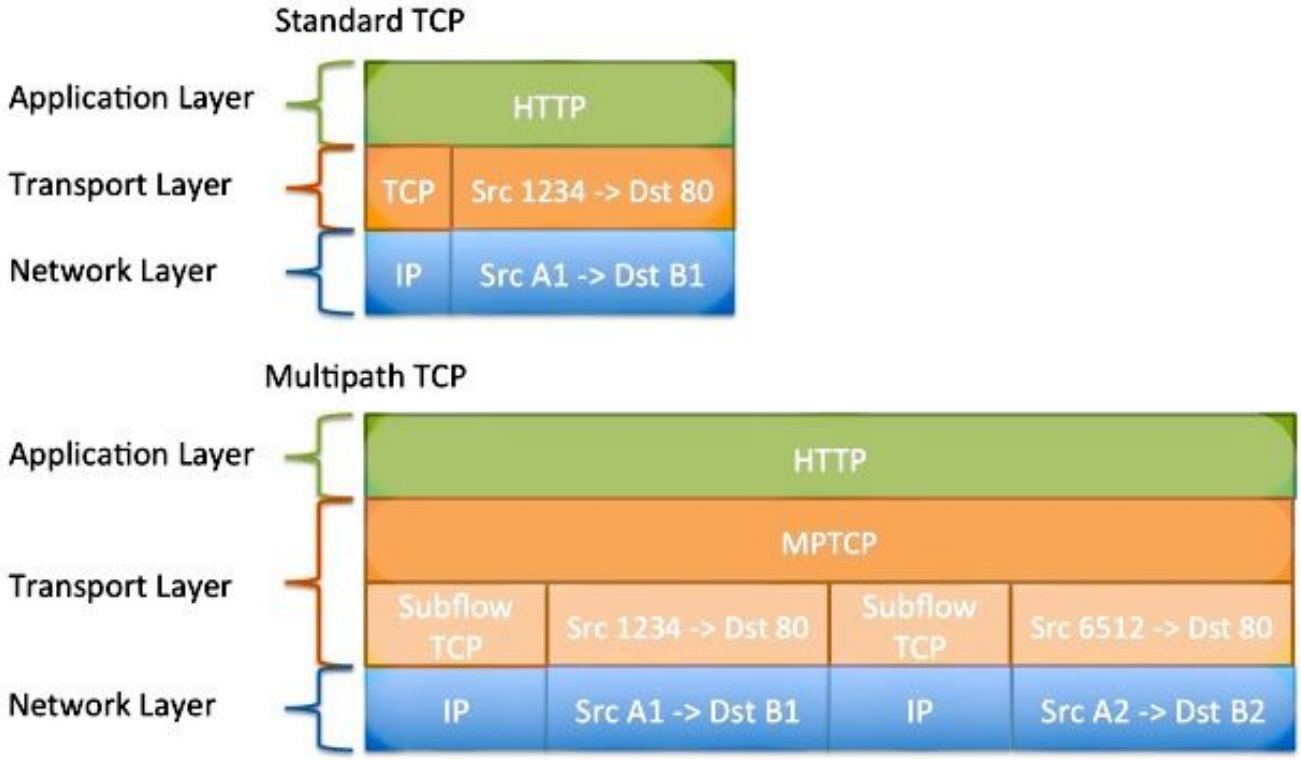
MPTCP は、単一のデータ フローが複数の接続に分割され実行できるようにする、通常の TCP の一連の拡張です。詳細については、RFC6824:TCP Extensions for Multipath Operation with Multiple Addresses を参照してください。

次の図に示すように、MPTCP は送信側のノードで 9 mbps のフローを 3 種類のサブフローに分

割することができます。これは受信側のノードで元のデータ フローに集約されます。



MPTCP 接続に参加するデータは、通常の TCP 接続を介した参加と同様に正しく機能します。つまり、送信されたデータは、順序どおりに配信されることが保証されています。MPTCP は、ネットワークのスタックを調整し、トランスポート層で動作するため、アプリケーションによって透過的に使用されます。

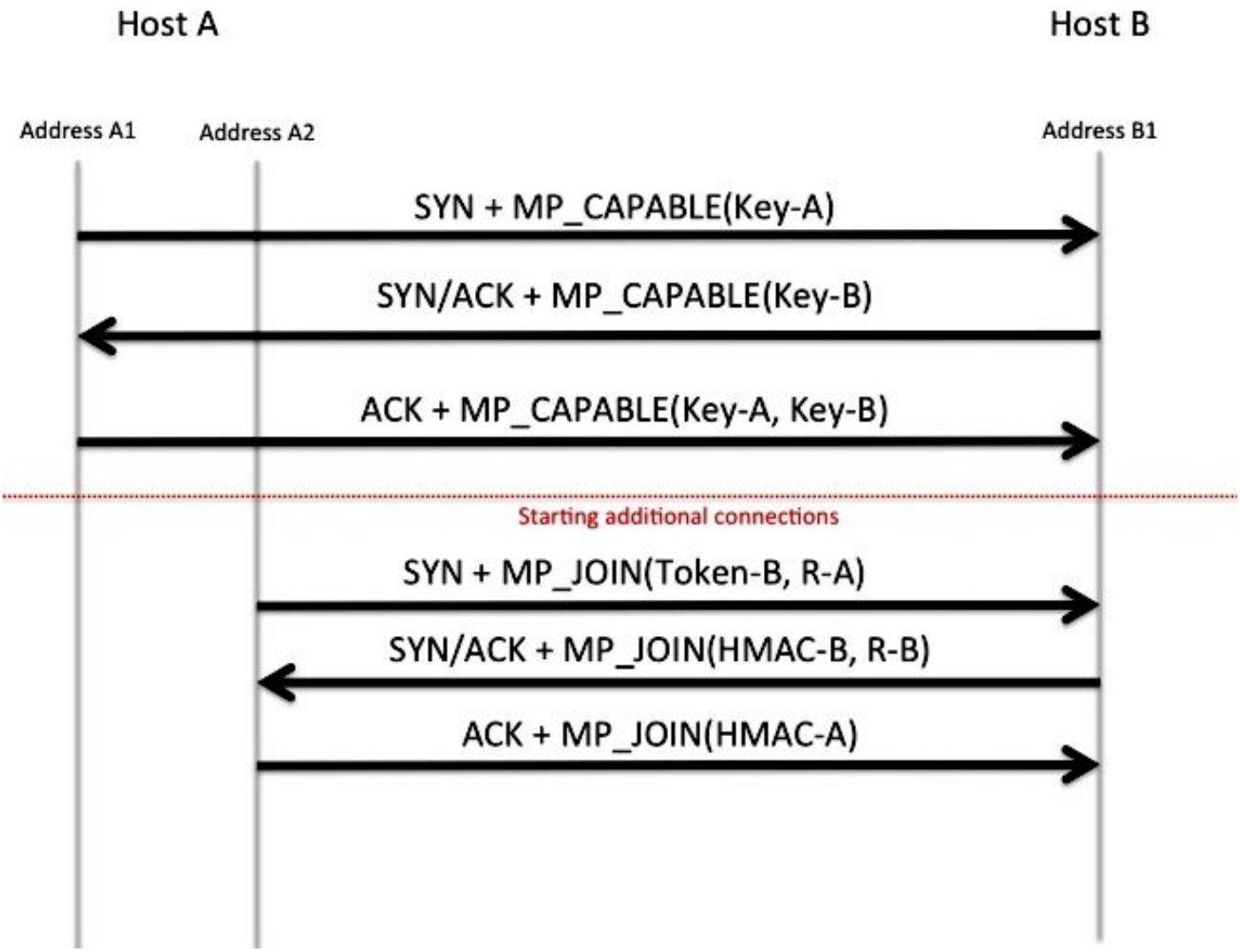


セッションの確立

MPTCP は、複数のサブ フローでのデータの分離と再構成をネゴシエートし、オーケストレーションするには、TCP オプションを使用します。**TCP オプション 30 は、MPTCP による包括的な使用のために Internet Assigned Numbers Authority (IANA) によって予約されています。**詳細については、Transmission Control Protocol (TCP) Parameters を参照してください。通常の TCP セッションの確立では、**MP_CAPABLE オプションは最初の同期 (SYN) パケットに含まれます。**応答側が MPTCP のネゴシエーションをサポートしていてこれを選択する場合は、SYN 許可 (ACK) パケットの **MP_CAPABLE オプションで応答します。**このハンドシェイク内で交換されるキーは、将来この MPTCP フローへの他の TCP セッションの参加および削除を認証するために使用されます。

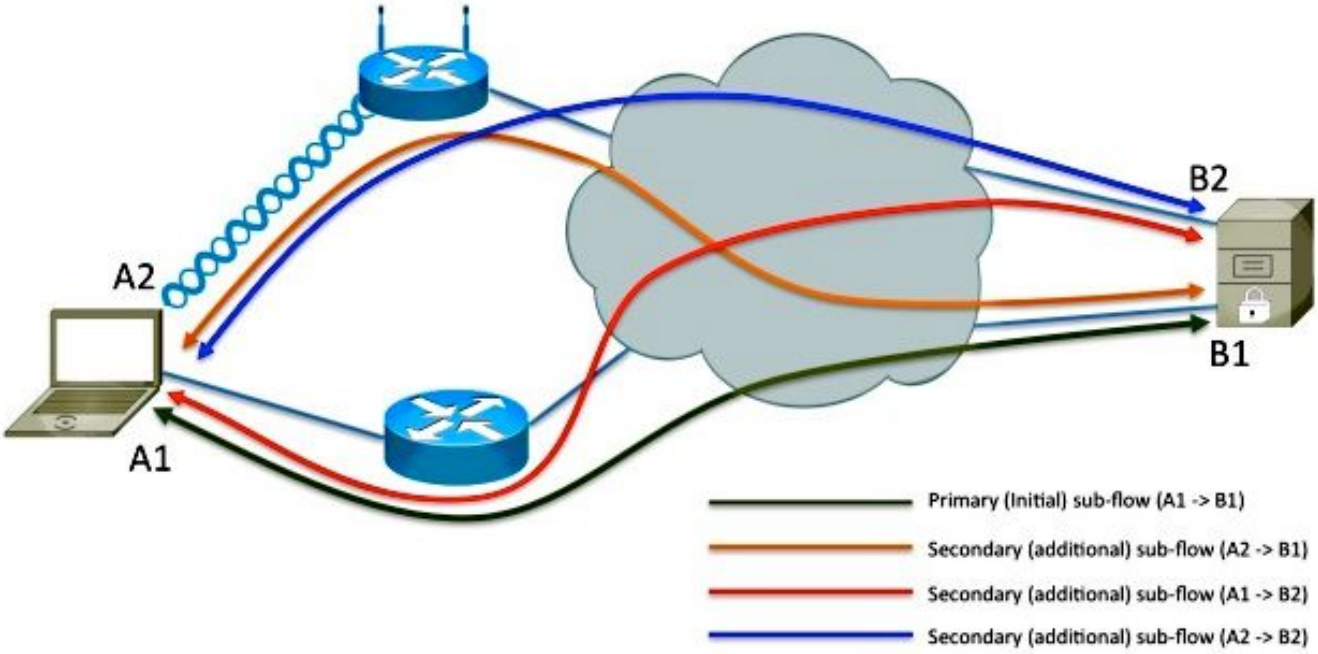
追加のサブフローの参加

必要であると思われる場合、**Host-A は Host-B** への別のインターフェイスまたはアドレスからの追加のサブフローを開始する場合があります。最初のサブフローと同様に、このサブフローをもう一方のサブフローにマージすることを指定するには、TCP オプションが使用されます。最初のサブフローの確立で（ハッシュ アルゴリズムとともに）交換するキーは、追加の要求が本当に**Host-A によって送信されていることを確認するために Host-B によって使用されます。**2 番目のサブフローの 4 タプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート）は最初のサブフローのものとは異なります。このフローはネットワークを介して異なるパスを実行する可能性があります。



アドレスの追加

Host-A に複数のインターフェイスがあり、Host-B に複数のネットワーク接続が存在する場合があります。Host-Bは、B1を宛先とする各アドレスからのHost-Aソーシングの結果、アドレスA1とA2について暗黙的に学習します。Host-Bは、追加アドレス(B2)をHost-Aにアドバタイズできます。これはTCPオプション3で完了します0.この図に示すように、Host-Bはセカンダリアドレス(B2)を**Host-A**にアドバタイズし、2つの追加のサブフローが作成されます。MPTCP がオープン システム相互接続（OSI）スタックのネットワーク層で動作するため、アドバタイズされる IP アドレスは、IPv4、IPv6、またはその両方の場合があります。一部のサブフローは、他のサブフローが IPv6 によって伝送されると、IPv4 で同時に伝送されることが可能です。



セグメンテーション、マルチパス、および再構成

アプリケーションが MPTCP に付与したデータ ストリームは、送信側が複数のサブフローにセグメント化して配信する必要があります。その後、このデータ ストリームをアプリケーションに再配信する前に、1 つのデータ ストリームに再構成する必要があります。

MPTCP は、各サブフローのパフォーマンスと遅延を調べ、最も高い総スループットを取得するにはダイナミックにデータの配信を調整します。データ転送時に、TCP ヘッダー オプションは、MPTCP のシーケンス番号と確認応答番号、現在のサブフロー シーケンス番号と確認応答番号、およびチェックサムに関する情報を含めます。

フロー検査の影響

多くのセキュリティデバイスは、ゼロアウトまたは不明なTCPオプションをNo Option(NOOP)値に置き換える可能性があります。ネットワーク デバイスが最初のサブフローで TCP SYN パケットにこれを実行すると、MP_CAPABLE アドバタイズメントは破棄されます。この結果、サーバはクライアントが MPTCP をサポートしていないと判断し、通常の TCP 動作に戻ります。

オプションが保持され、MPTCPが複数のサブフローを確立できる場合、ネットワークデバイスによるインラインパケット分析が確実に機能しない可能性があります。これはデータ フローの一部だけが各サブフローに引き継がれるためです。MPTCP へのプロトコル インスペクションの影響は、何もない場合もあればサービスが完全に中断される場合もあります。影響は検査するデータの内容と程度によって変わってきます。パケット分析には、ファイアウォールアプリケーション層ゲートウェイ（ALGまたはフィックスアップ）、ネットワークアドレス変換(NAT)ALG、Application Visibility and Control(AVC)、Network Based Application Recognition(NBAR)または侵入検知サービス(IDS/IPS)などがあります。 アプリケーション インスペクションが環境に必要な場合、**TCP オプション 30 の削除をイネーブルにすることを推奨します。**

暗号化が原因でフローが検査されない場合、あるいはプロトコルが不明な場合は、インライン装置の MPTCP フローへの影響はありません。

MPTCP の影響を受けるシスコ製品

次の製品は MPTCP による影響を受けます：

- 適応型セキュリティ アプライアンス（ASA）
- Cisco Firepower Threat Defense
- 侵入防御システム（IPS）
- Cisco IOS-XEおよびIOS®
- Application Control Engine（ACE）

各製品は、このドキュメントの後の項で詳細に説明します。

ASA

TCP の動作

デフォルトでは、Cisco ASA ファイアウォールは、**MPTCP オプション 30** などのサポートされていない TCP オプションを NOOP オプション（オプション 1）と置き換えます。 MPTCP オプションを許可するには、次の設定を使用します：

1. デバイスから **TCP オプション 30（MPTCP で使用）を許可するポリシーを定義します：**

```
tcp-map my-mptcp
   tcp-options range 30 30 allow
```

2. トラフィックの選択を定義します：

```
class-map my-tcpnorm
   match any
```

3. トラフィックからアクションへのマップを定義します：

```
policy-map my-policy-map
   class my-tcpnorm
       set connection advanced-options my-mptcp
```

4. ボックスまたはインターフェイスごとにこれをアクティブ化します：

```
service-policy my-policy-map global
```

プロトコル インスペクション

ASA は多くのプロトコルのインスペクションをサポートしています。インスペクション エンジンのアプリケーションへの影響は異なります。インスペクションが必要な場合、上記の TCP マップを適用しないことを推奨します。

Cisco Firepower Threat Defense

TCP の動作

FTDはIPS/IDSサービスに対してディープパケットインスペクションを実行するため、TCPオプションが通過できるようにtcp-mapを変更することは推奨されません。

Cisco IOS ファイアウォール

コンテキストベース アクセス コントロール（CBAC）

CBACは、TCPストリームからTCPオプションを削除しません。MPTCP は、ファイアウォールを経由して接続を作成します。

ゾーンベース ファイアウォール（ZBFW）

Cisco IOSおよびIOS-XE ZBFWは、TCPストリームからTCPオプションを削除しません。MPTCP は、ファイアウォールを経由して接続を作成します。

ACE

デフォルトでは、ACE デバイスは TCP 接続から TCP オプションを排除します。MPTCP 接続は、通常の TCP 動作にフォールバックします。

ACEデバイスは、**tcp-optionsコマンドを使用してTCPオプションを許可するように設定できます**。詳細については、『セキュリティガイドvA5(1.0)』の「ACEによるTCPオプションの処理方法」セクションを参照してください。ただし、2 番目のサブフローが異なる実サーバに分散されて、接続が失敗する場合があるので、これが常に推奨されるわけではありません。

MPTCP によって影響を受けないシスコ製品

一般に、TCPフローやレイヤ7情報を検査しないデバイスはTCPオプションを変更しないため、その結果MPTCPに対して透過的になります。これらのデバイスには次のようなものがあります：

- Cisco 5000 シリーズ ASR（Starent）
- Wide Area Application Services（WAAS）
- キャリアグレードの NAT（CGN）（Carrier Routing System（CRS）のキャリアグレードのサービス エンジン（CGSE）ブレード）
- すべてのイーサネット スイッチ製品
- すべてのルータ製品（ファイアウォールまたは NAT 機能がイネーブルになっていない場合。詳細については、ドキュメントの前半にある「MPTCPの影響を受けるシスコ製品」の項を参照してください)